



**U.S. Department of Justice**  
**Immigration and Naturalization Service**

40/11.2.4

*1200 Mercantile Lane, Suite 115  
Largo, MD 20774*

May 15, 2000

Information Technology Laboratory  
Attn: AES Finalist Comments (Bldg. 820, Room 423)  
National Institute of Standards and Technology  
100 Bureau Drive, STOP 8930  
Gaithersburg, MD 20899-8930  
U.S.A.

**Subject: INS HQRSS AES Finalist Comments and Recommendations**

Dear Sir/Madam:

The Immigration and Naturalization Service (INS) Headquarters Radio Systems Section (HQRSS) is pleased to submit comments and recommendations concerning the Advanced Encryption Standard (AES).

**INS BACKGROUND**

As the largest Federal law enforcement agency, the INS operates one of the most extensive civilian law enforcement wireless communications systems in the world operating in the HF, VHF, UHF, and microwave bands. INS HQRSS is responsible for the design, engineering, implementation, and operation and maintenance of the INS' wireless communications systems Service-wide.

Currently, the INS' wireless communications systems support the operational communications requirements of over 17,000 INS law enforcement personnel in urban, suburban, and rural areas. The INS provides wireless communications throughout the continental United States, Alaska, Hawaii, Guam, and Puerto Rico. INS law enforcement personnel are distributed throughout three (3) Regions, 21 Sectors, and 36 Districts. These INS agents/officers staff over 250 air, land, and sea ports of entry and patrol over 8,000 miles of international boundaries in land vehicles, aircraft, or boats, as well as on horseback or on foot. In addition, the INS operates ten (10) detention facilities known as Service Processing Centers (SPCs).

The INS has over 17,000 handheld/portable radios and over 15,000 mobile/vehicular radios that support both INS personnel and multi-agency task forces comprised of Federal, state, and local law enforcement personnel. These 32,000 radios operate over a nationwide wireless communications systems consisting of approximately 1,400 base stations/mobile relay/repeater stations.

The INS has an extensive wireless communications infrastructure that includes, but is not limited to: VHF and UHF mobile relay/repeaters, satellite voting receivers, command and control (C2) centers, microwave backbone infrastructure, base stations, control base stations, HF stations, antennas, towers, shelters, etc.

The INS has deployed and continues to deploy cryptographically protected narrowband digital wireless equipment as part of its Encrypted Voice Radio Program (EVRP) and now as part of the Justice Wireless Network (JWN).

INS communications system are protected by both Type 1 and Type 3 cryptographic algorithms. As the AES is intended to become the standard for future Type-3 usage, the INS has a significant interest in the outcome of the AES process.

The following are the INS' comments and recommendations on the AES finalist:

#### **INS RECOMMENDED AES ALGORITHM**

The INS is convinced by the security argument that a very conservative cipher design, employing a large security margin, is needed for the selection of the AES. Based upon our review of the published documentation, the TWOFISH algorithm appears to have the most conservative design and possesses the great security margin.

Notwithstanding the apparent attributes of TWOFISH, NIST is also concerned that the AES finalist will be able to sustain attacks from future, unknown attacks. It is the INS' belief that the most credible way to ensure the integrity of an algorithm is to further increase its security margin vis-à-vis an increased number of rounds and through the selection of a maximal key variable length.

In addition, the underpinnings of successful cipher implementation depends to a large extent upon the selection of an appropriate random number generator (RNG). The INS strongly encourages AES implementations to embrace a suitable, secure RNG.

Therefore, the INS recommends the selection of the TWOFISH algorithm as the AES, with the following caveats:

- (a) As security considerations are paramount to the INS, the INS recommends the adoption of TWOFISH with a mandatory 256-bit traffic key. Traffic key lengths less than 256 bits should be prohibited.
- (b) The INS recommends that TWOFISH be adopted with an increased number of rounds from the current 16 to a minimum of 20 with 24 rounds recommended.

Given the current trends in microelectronics, the INS believes that mandating a 256 bit key length and increasing the number of rounds to either 20 or 24 will have a negligible effect on future products that will be employing the AES while going a long way to ensuring the algorithms ultimate long term credibility.

## **ELECTRONIC CRYPTOGRAPHIC KEY DISTRIBUTION**

### ***Over-The-Air-Rekey (OTAR)***

The INS and other law enforcement agencies makes extensive use of electronic cryptographic key management and distribution techniques in its cryptographically protected systems. Cryptographically protected INS wireless equipment has its cryptographic traffic key variables changed by means of an Over-The-Air-Rekey (OTAR) protocol. The OTAR process currently employed by INS, (and other law enforcement agencies) in its EVRP systems are not based upon ANSI X9.17 or ANSI X9.42, but rather is optimized for the unique environment that characterizes wireless communications. The OTAR protocol for Type-1, 2, 3 and 4 cryptographically protected, tactical law enforcement communications is specified in the TIA/EIA APCO Project 25 series of international law enforcement wireless communications standards.

This Project 25-compliant OTAR protocol, is defined in the TIA/EIA APCO Project 25 Over-The-Air-Rekeying (OTAR) Protocol document, TSB102.AACA. This Project 25 international law enforcement wireless communications standard is likewise not based upon either ANSI X9.17 or ANSI X9.42.

### ***Recommendation - OTAR***

The INS recommends that NIST recognize and permit continued use of existing OTAR protocols, such as that currently employed by the INS, and that the TSB102.AACA Project 25 OTAR protocol be referenced for use in wireless communications systems that make use of the AES.

## **RANDOM NUMBER GENERATION:**

The selection of an appropriate, secure RNG is fundamental to any effective AES implementation.

### ***Recommendation - RNG***

The INS recommends that NIST specify an appropriate and secure RNG for use with the AES.

**NIST Question 1: How many AES Algorithms?**

***INS Response:***

The INS recommends NIST select a single AES algorithm. The INS is particularly concerned with communications interoperability. The selection of a single AES algorithm will promote communications and cryptographic interoperability.

**NIST Question 2: What about the speed versus security margin tradeoff?**

***INS Response:***

The INS assessment is that technology both currently available, and to be available, nullifies any speed versus security trade off.

In addition, it is well known that "speed" is often more a function of the efficiency of the code and of the compiler employed. Thus, it is possible that an algorithm that was the "fastest" could be poorly implemented and thus exhibits slow speed. Conversely, an algorithm that was not the fastest could be implemented in a highly efficient fashion and actually is "faster" than believed.

The INS position is that cryptographic security and integrity are paramount in the selection of the AES.

**NIST Question 3: How important are low-end smart cards and related environments when selecting the AES algorithm(s)?**

***INS Response:***

As with Question 2, the INS assessment is that both currently available and to be available technology will nullify any argument tied to the use of low-end smart cards.

Smart card technology is advancing and the smart cards of today are likely to be eclipsed by the smart cards of tomorrow.

The fundamental issue is preserving the integrity of the data involved and again cryptographic strength is the primary determinate. The microelectronics industry continues to flourish with innovation that will address the hardware, software and power needs of the selected AES algorithm.

**Question 4: What is the relative importance of hardware vs. software performance in the selection of the AES algorithm?**

***INS Response:***

The INS believes that software and hardware vendors will optimize their processes to make effective use of the algorithm that is selected as the AES. Notwithstanding this, the INS is practically concerned with the following issues:

- (a) Implementation Power Consumption
- (b) RAM
- (c) Key Agility

Assuming the cryptographic security provided by an algorithm were equivalent, the algorithm with the lowest power consumption, least RAM usage, and most efficient Key Agility mechanism should be selected.

The INS position is that cryptographic security and integrity are paramount in the selection of the AES.

**NIST Question 5: What modes of operation should be available for the AES algorithm?**

***INS Response:***

The INS strongly believes that flexibility concerning cryptographic mode implementation should be afforded, provided that security is not compromised.

The INS recommends that NIST not endorse/approve any cryptographic implementations that are inherently nonsecure, for example, 1 bit OFB. In this regard the INS further recommends that NIST promulgate implementation guidelines that will help ensure that products which employ the AES, in either software or hardware, afford effective cryptographic protection.

The INS is concerned that certain AES implementations may not guarantee key stream length. In this regard, the INS is particularly interested in the AES permitting 128 bit Output Feed Back (128 bit OFB) and 128 bit Counter-Addressing (also referred to as the Long Cycle or Linear Regression mode).

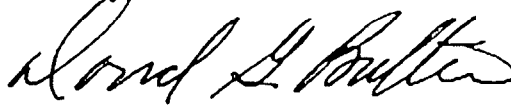
**SCHEDULE**

As a final comment, the INS applauds NIST's efforts with respect to the AES. The INS is anxious to make use of the AES and encourages NIST to move forward with the AES process in the most expedient fashion possible.

Upon selection of the AES, the INS recommends NIST immediately promulgate interim guidelines on the AES to promote rapid development of AES based products.

Thank you for the opportunity to submit comments on this critically important subject. Should you have any questions, please contact Dr. Gregory M. Stone on 301.925.9773.

Sincerely,

A handwritten signature in black ink, appearing to read "David G. Butler". The signature is fluid and cursive, with the first name "David" being the most prominent.

David G. Butler  
Chief  
Radio Systems Section